

# Integral Solutions to Linear Indeterminate Equation

CHANGJIANG ZHU

The Hubei Key Laboratory of Mathematical Sciences,  
School of Mathematics and Statistics,  
Huazhong Normal University, Wuhan 430079, P.R. China.

**Abstract:** In this paper, using Euler's function, we give a formula of all integral solutions to linear indeterminate equation with  $s$ -variables  $a_1x_1 + a_2x_2 + \cdots + a_sx_s = n$ . It is a explicit formula of the coefficients  $a_1, a_2, \cdots, a_s$  and the free term  $n$ .

**Key words:** Linear indeterminate equation, Euler's function, integral solution.

**2000 AMS Subject Classification:** 11D04, 11D72.

## 1. Introduction and Main Theorem

In this paper, we consider the integral solutions to linear indeterminate equation with  $s$ -variables

$$a_1x_1 + a_2x_2 + \cdots + a_sx_s = n. \quad (1.1)$$

It is well-known that there exist the integral solutions of (1.1) if and only if

$$(a_1, a_2, \cdots, a_s) | n. \quad (1.2)$$

Under the assumption (1.2), if we can obtain a special solution of (1.1) by applying the mutual division, fraction, parameter methods, etc., then the all integral solutions to (1.1) can be represented by using the special solution obtained above and  $s-1$  parameters  $t_1, t_2, \cdots, t_{s-1}$ . However, the methods seeking above special solution are too complicated to lose availability in many problems. For example, it is very difficult to obtain a special solution to the following simple indeterminate equation with  $s = 2$

$$2^m x + 3^n y = 1, \quad (1.3)$$

where  $m$  and  $n$  are positive integers. Therefore, it is very important and interesting to seek a formula of all integral solutions to (1.1). In this paper, using Euler's function, we give a formula of all integral solutions to (1.1), which is a explicit function of the coefficients  $a_1, a_2, \cdots, a_s$  and the free term  $n$ .

To state our result, let  $(a_1, a_2, \dots, a_s) = d$ ,  $n = dn_1$ ,  $(a_1, a_2) = d_2$ ,  $(d_2, a_3) = d_3$ ,  $\dots$ ,  $(d_{s-1}, a_s) = d_s = d$ ,  $a_1 = d_2 \bar{a}_1$ ,  $a_2 = d_2 \bar{a}_2$ ,  $\dots$ ,  $a_s = d_s \bar{a}_s$ ,  $d_2 = d_3 \bar{d}_2$ ,  $d_3 = d_4 \bar{d}_3$ ,  $\dots$ , and  $d_{s-1} = d_s \bar{d}_{s-1}$ .

Then

$$(\bar{a}_1, \bar{a}_2) = 1, \quad (\bar{d}_i, \bar{a}_{i+1}) = 1, \quad i = 2, 3, \dots, s-1.$$

Also we appoint

$$\bar{a}_1 = \bar{d}_1, \quad \sum_{i=j}^k (\cdot) = 0, \quad \text{if } k < j$$

and

$$\prod_{i=j}^{j-\lambda} (\cdot) = \begin{cases} 1, & \lambda = 1, \\ 0, & \lambda \geq 2. \end{cases}$$

**Theorem 1.1. (Main Theorem)** *If  $(a_1, a_2, \dots, a_s) | n$ , then all integral solutions to the indeterminate equation (1.1) have the following forms:*

$$\left\{ \begin{array}{l} x_1 = n_1 \prod_{i=1}^{s-1} \bar{d}_i^{\phi(|\bar{a}_{i+1}|)-1} + \sum_{m=1}^{s-1} \bar{a}_{m+1} \prod_{i=1}^{m-1} \bar{d}_i^{\phi(|\bar{a}_{i+1}|)-1} t_m, \\ x_k = \frac{n_1}{\bar{a}_k} \left( 1 - \bar{d}_{k-1}^{\phi(|\bar{a}_k|)} \right) \prod_{i=k}^{s-1} \bar{d}_i^{\phi(|\bar{a}_{i+1}|)-1} - \bar{d}_{k-1} t_{k-1} \\ \quad + \sum_{m=2}^{s-1} \frac{\bar{a}_{m+1}}{\bar{a}_k} \left( 1 - \bar{d}_{k-1}^{\phi(|\bar{a}_k|)} \right) \prod_{i=k}^{m-1} \bar{d}_i^{\phi(|\bar{a}_{i+1}|)-1} t_m, \\ \quad \quad \quad k = 2, 3, \dots, s, \end{array} \right. \quad (1.4)$$

where  $t_1, t_2, \dots, t_{s-1}$  are arbitrary integers.

## 2. The Proof of Theorem 1.1

To prove our Theorem 1.1, we restate the following Euler's lemma, which is required in later analysis.

**Lemma 2.1** (Euler's Lemma [2, 3, 5]). *Let  $(a, b) = 1$ . Then*

$$b \mid \left( 1 - a^{\phi(|b|)} \right), \quad (2.1)$$

and

$$a \mid \left( 1 - b^{\phi(|a|)} \right), \quad (2.2)$$

where  $\phi(\cdot)$  denotes Euler's function.

To study the indeterminate equation (1.1), we first discuss a simple case of (1.1) with  $s = 2$ .

**Lemma 2.2.** *For the indeterminate equation*

$$ax + by = c, \quad (2.3)$$

*if  $(a, b) | c$ , then all integral solutions to (2.3) have the following forms:*

$$\begin{cases} x = c_0 a_0^{\phi(|b_0|)-1} + b_0 t, \\ y = \frac{c_0}{b_0} \left(1 - a_0^{\phi(|b_0|)}\right) - a_0 t \end{cases} \quad (2.4)$$

*or*

$$\begin{cases} x = \frac{c_0}{a_0} \left(1 - b_0^{\phi(|a_0|)}\right) - b_0 t, \\ y = c_0 b_0^{\phi(|a_0|)-1} + a_0 t, \end{cases} \quad (2.5)$$

*where  $a_0 = \frac{a}{(a,b)}$ ,  $b_0 = \frac{b}{(a,b)}$ ,  $c_0 = \frac{c}{(a,b)}$ ,  $t = 0, \pm 1, \pm 2, \dots$ .*

*Proof.* Without the loss of generality, we only prove (2.4). The proof of (2.5) is similar and the details are omitted. In fact, using Lemma 2.1, it is easy to verify that  $(x, y)$  is a integral solution to (2.2). On the other hand, let  $(x_0, y_0)$  be a integral solution to (2.2), i.e.,

$$ax_0 + by_0 = c. \quad (2.6)$$

Then

$$a_0 x_0 + b_0 y_0 = c_0, \quad (2.7)$$

where  $(a_0, b_0) = 1$ , which implies

$$a_0 x_0 \equiv c_0 \pmod{|b_0|}. \quad (2.8)$$

Therefore,  $x \equiv x_0 \pmod{|b_0|}$  must be the solution of (2.8).

Noticing (2.8) has a unique solution

$$x \equiv a_0^{\phi(|b_0|)-1} c_0 \pmod{|b_0|},$$

it follows

$$x_0 \equiv a_0^{\phi(|b_0|)-1} c_0 \pmod{|b_0|}.$$

This shows that there exists a  $t_0 \in \{0, \pm 1, \pm 2, \dots\}$ , such that

$$x_0 = c_0 a_0^{\phi(|b_0|)-1} + b_0 t_0. \quad (2.9)$$

Substituting (2.9) into (2.7), we have

$$a_0 \left( c_0 a_0^{\phi(|b_0|)-1} + b_0 t_0 \right) + b_0 y_0 = c_0, \quad (2.10)$$

which implies

$$y_0 = \frac{c_0}{b_0} \left(1 - a_0^{\phi(|b_0|)}\right) - a_0 t_0. \quad (2.11)$$

(2.9) and (2.10) show that every solution  $(x_0, y_0)$  to equation (2.3) satisfies (2.4).

The proof of Lemma 2.2 is completed.

Now we will seek a formula of all integral solutions to (1.1). To do this,

*Proof of Theorem 1.1.* First, we prove that  $(x_1, x_2, \dots, x_s)$  defined by (1.4) is a integer solution to (1.1). By using Lemma 1.1, we know that  $x_1, x_2, \dots, x_s$  defined by (1.4) are integers. Moreover, since

$$\begin{aligned} n_1 a_1 &= n_1 \bar{d}_1 d_2 = n_1 \bar{d}_1 \bar{d}_2 d_3 = \dots = n_1 \bar{d}_1 \bar{d}_2 \dots \bar{d}_{s-1} d_s = n \bar{d}_1 \bar{d}_2 \dots \bar{d}_{s-1}, \\ n_1 a_k &= n_1 \bar{a}_k d_k = n_1 \bar{a}_k \bar{d}_k d_{k+1} = \dots = n_1 \bar{a}_k \bar{d}_k \dots \bar{d}_{s-1} d_s = n \bar{a}_k \bar{d}_k \dots \bar{d}_{s-1}, \\ k &= 2, 3, \dots, s-1, \end{aligned}$$

and

$$n_1 a_s = n_1 \bar{a}_s d_s = n \bar{a}_s,$$

we have

$$\begin{aligned} a_1 n_1 \prod_{i=1}^{s-1} \bar{d}_i^{(\lceil \bar{a}_{i+1} \rceil - 1)} + a_2 \frac{n_1}{\bar{a}_2} \left(1 - \bar{d}_1^{(\lceil \bar{a}_2 \rceil)}\right) \prod_{i=2}^{s-1} \bar{d}_i^{(\lceil \bar{a}_{i+1} \rceil - 1)} + \dots \\ + a_{s-1} \frac{n_1}{\bar{a}_{s-1}} \left(1 - \bar{d}_{s-2}^{(\lceil \bar{a}_{s-1} \rceil)}\right) \prod_{i=s-1}^{s-1} \bar{d}_i^{(\lceil \bar{a}_{i+1} \rceil - 1)} + a_s \frac{n_1}{\bar{a}_s} \left(1 - \bar{d}_{s-1}^{(\lceil \bar{a}_s \rceil)}\right) = n, \end{aligned} \quad (2.12)$$

$$a_1 \bar{a}_2 t_1 - a_2 \bar{d}_1 t_1 = \bar{d}_1 d_2 \bar{a}_2 t_1 - \bar{a}_2 d_2 \bar{d}_1 t_1 = 0, \quad (2.13)$$

and

$$\begin{aligned} a_1 \bar{a}_{m+1} \prod_{i=1}^{m-1} \bar{d}_i^{(\lceil \bar{a}_{i+1} \rceil - 1)} t_m + a_2 \frac{\bar{a}_{m+1}}{\bar{a}_2} \left(1 - \bar{d}_1^{(\lceil \bar{a}_2 \rceil)}\right) \prod_{i=2}^{m-1} \bar{d}_i^{(\lceil \bar{a}_{i+1} \rceil - 1)} t_m \\ + \dots + a_{m-1} \frac{\bar{a}_{m+1}}{\bar{a}_{m-1}} \left(1 - \bar{d}_{m-2}^{(\lceil \bar{a}_{m-1} \rceil)}\right) \prod_{i=m-1}^{m-1} \bar{d}_i^{(\lceil \bar{a}_{i+1} \rceil - 1)} t_m \\ + a_m \frac{\bar{a}_{m+1}}{\bar{a}_m} \left(1 - \bar{d}_{m-1}^{(\lceil \bar{a}_m \rceil)}\right) t_m - a_{m+1} \bar{d}_m t_m = 0, \\ m = 2, 3, \dots, s-1. \end{aligned} \quad (2.14)$$

Adding both sides of (2.12), (2.13) and (2.14), we have

$$a_1 x_1 + a_2 x_2 + \dots + a_s x_s = n,$$

which implies  $(x_1, x_2, \dots, x_s)$  defined by (1.4) is a integral solution to (1.1).

On the other hand, we will prove that every integral solution to (1.1) can be represented into form (1.4) by using induction for  $s$ .

For  $s = 2$ , it is true by Lemma 2.2.

Suppose that it is true for the indeterminate equation of  $s - 1$  variables, i.e., the every solution of

$$a_1 x_1 + a_2 x_2 + \dots + a_{s-1} x_{s-1} = n$$

can be represented into form (1.4). Now we will show that it is true for  $s$ .

Since  $d_{s-1} | (a_1 x_1 + a_2 x_2 + \dots + a_{s-1} x_{s-1})$ , there exists  $y_{s-1}$  such that

$$a_1 x_1 + a_2 x_2 + \dots + a_{s-1} x_{s-1} = d_{s-1} y_{s-1}. \quad (2.15)$$

(1.1) and (2.15) show

$$d_{s-1}y_{s-1} + a_s x_s = n. \quad (2.16)$$

From Lemma 2.2 and the inductive assumption, we have

$$x_1 = y_{s-1} \prod_{i=1}^{s-2} \bar{d}_i^{\phi(|\bar{a}_{i+1}|)-1} + \sum_{m=1}^{s-2} \bar{a}_{m+1} \prod_{i=1}^{m-1} \bar{d}_i^{\phi(|\bar{a}_{i+1}|)-1} t_m, \quad (2.17)$$

$$\begin{aligned} x_k &= \frac{y_{s-1}}{\bar{a}_k} \left( 1 - \bar{d}_{k-1}^{\phi(|\bar{a}_k|)} \right) \prod_{i=k}^{s-2} \bar{d}_i^{\phi(|\bar{a}_{i+1}|)-1} - \bar{d}_{k-1} t_{k-1} \\ &\quad + \sum_{m=2}^{s-2} \frac{\bar{a}_{m+1}}{\bar{a}_k} \left( 1 - \bar{d}_{k-1}^{\phi(|\bar{a}_k|)} \right) \prod_{i=k}^{m-1} \bar{d}_i^{\phi(|\bar{a}_{i+1}|)-1} t_m, \\ &\quad k = 2, 3, \dots, s-1, \end{aligned} \quad (2.18)$$

$$y_{s-1} = n_1 \bar{d}_{s-1}^{\phi(|\bar{a}_s|)-1} + \bar{a}_s t_{s-1}, \quad (2.19)$$

and

$$x_s = \frac{n_1}{\bar{a}_s} \left( 1 - \bar{d}_{s-1}^{\phi(|\bar{a}_s|)} \right) - \bar{d}_{s-1} t_{s-1}. \quad (2.20)$$

Substituting (2.19) into (2.17), (2.18) and noticing (2.20), we know every integral solution to (1.1) can be represented into form (1.4).

This completes the proof of Theorem 1.1.

**Remark 2.4.** *The formula (1.4) of all integral solutions in Theorem 2.3 was deduced from the first group formula (2.4) of Lemma 2.2. If we use the second group formula (2.5) to solve the indeterminate equation (1.1), we can obtain the other formula with different form of all integral solutions to (1.1).*

### 3. Applications

In this section, we will solve the indeterminate equation (1.3) by using Theorem 1.1. To do this, we first give Euler's functions  $\phi(2^m)$  and  $\phi(3^n)$  as follows:

$$\begin{cases} \phi(2^m) = 2^m - 2^{m-1}, \\ \phi(3^n) = 3^n - 3^{n-1}. \end{cases} \quad (3.1)$$

By applying Theorem 1.1, the all integral solutions to (1.3) can be represented into the following forms:

$$\begin{cases} x = 2^{m(3^n - 3^{n-1} - 1)} + 3^n t, \\ y = \frac{1}{3^n} \left( 1 - 2^{m(3^n - 3^{n-1})} \right) - 2^m t \end{cases} \quad (3.2)$$

or

$$\begin{cases} x = \frac{1}{2^m} \left( 1 - 3^{n(2^m - 2^{m-1})} \right) - 3^n t, \\ y = 3^{n(2^m - 2^{m-1} - 1)} + 2^m t, \end{cases} \quad (3.3)$$

where  $t = 0, \pm 1, \pm 2, \dots$ .

**Acknowledgement:** The research was supported by the Natural Science Foundation of China #10625105, #11071093, the PhD specialized grant of the Ministry of Education of China #20100144110001, and the Special Fund for Basic Scientific Research of Central Colleges #CCNU10C01001.

## References

- [1] Apostol, T.M., Introduction to Analytic Number Theory, Springer-Verlag, Berlin, Heidelberg, New York, 1976.
- [2] Dudley, U., Elementary Number Theory, W.H. Freeman and Company, New York, 1978.
- [3] Gareth, A. Jones and J. Mary Jones, Elementary Number Theory, Springer-Verlag, Berlin, Heidelberg, New York, 1978.
- [4] Hardy, G.H. and Wright, E.M., An Introduction to the Theory of Numbers, Oxford University Press, Walton Street, Oxford OX2 6DP, 1979.
- [5] Hua, L.G., Introduction to Number Theory, Springer-Verlag, Berlin, Heidelberg, New York, 1982.
- [6] Kenneth Ireland and Michael Rosen, A Classical Introduction to Modern Number Theory, Springer-Verlag, Berlin, Heidelberg, New York, 1990.
- [7] Mathews, G.B., Theory of Numbers, New York: Chelsea Publishing, 1961.
- [8] Redmond, D., Number Theory: An Introduction, New York: Marcel Dekker, c1996.
- [9] Schmidt, W.M., Diophantine Approximations and Diophantine Equations, Lecture Notes in Math., Vol. 1467, Springer-Verlag, Berlin, Heidelberg, New York, 1991.